

Appl. No. 09/773,665
Reply to Office Action of: September 12, 2005

REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Claim Amendments

Applicant advises that claim 12 is amended to correct a typographical error, namely replacing "pairs" with "pair" on line 12 of claim 12. No new subject matter is believed to have been added by way of this amendment.

Claim Rejections – 35 U.S.C. § 103

Claims 12-21 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Applied Cryptography by Schneier ("Schneier") in view of the article "New Public-Key Schemes Based on Elliptic Curves over the Ring Z_n " by Koyama ("Koyama"). Applicant respectfully traverses the rejections as follows.

Claim 12 is directed to a method for verifying a signature for a message m and requires a sender generating masked signature components (r, s, c) . The component r is an integer derived from a coordinate of a first short term public key kP . The component s is a signature component derived by binding a second short term private key, the message m , and short and long term private keys. The component c is a second signature component obtained by combining the first and second short term private keys. This set of components (r, s, c) is used by the verifier for verifying the signature. This is clearly recited in the preamble of claim 1.

In claim 12, the verifier first obtains a pair of signature components (\bar{s}, r) , where \bar{s} is derived from the first and second signature components, namely s and c , the nature of s and c being described above. The verifier then recovers a coordinate pair (x_1, y_1) , which corresponds to the first short term public key kP . This coordinate pair is recovered using the pair (\bar{s}, r) and the message m . The verifier then calculates a signature component r' from one of the coordinate pair, and then verifies that $r' = r$, where r was originally included in the pair (\bar{s}, r) .

Applicant respectfully submits that the Examiner has misconstrued the teachings of Schneier, and will show that Schneier fails to teach what is recited in claim 12. Moreover, the

Appl. No. 09/773,665
Reply to Office Action of: September 12, 2005

additional teachings taken from Koyama fail to provide what is missing from Schneier and in fact provides no direction or motivation for applying the teachings to Schneier, and thus are entirely inapplicable.

The Examiner relies on a passage in pages 509-510 of Schneier. This passage outlines the Guillou-Quisquater Signature Scheme, where Alice computes signature components d and D as $d = H(M, T)$ and $D = rB^d \bmod n$ respectively. The component T is computed using a random integer r , and the function H is a hash function. Alice sends the components d and D along with the message M and her credentials j to Bob. Bob uses d and D to compute a representation of the component T , namely T' and then calculates a representation of d , namely d' using the message M and the representation T' . Bob then verifies the signature by comparing d with d' .

Firstly, the Examiner has equated the components d and D with the components (\bar{s}, r) , and further states that "said component being derived from a first (random integer r) and second signature components (B) generated by a signor...". Applicant believes that the Examiner has not fully considered the nature of (\bar{s}, r) recited in claim 12. For instance, \bar{s} in claim 12 is derived from components s and c , which are derived as outlined above (and clearly recited in the preamble of claim 12). However, neither component d nor component D are derived in such a way. For example, component d is derived from a message M and component T . Although the component s is derived in part from the message m , there is no teaching in Schneier that would lead a person skilled in the art to believe that the component T is equivalent to the second short term private key and short and long term public keys. Schneier is entirely silent in that regard. Therefore, \bar{s} and d are completely different and thus, Applicant submits, cannot be considered equivalent.

Similarly, the component D is derived from the integer r and the component d . Clearly this is not equivalent to how \bar{s} is derived. In claim 12, component c is derived from the first and second short term private keys. A careful review of Schneier will reveal that there is no mention of deriving a signature component in such a way. Equating D in Schneier to either \bar{s} or r is believed to be improper and cannot be considered equivalent components.

Schneier also does not teach obtaining a pair of signature components from a set of three components as recited in claim 12. Schneier simply does not teach utilizing masked signature components such as (r, s, c) recited in claim 12. In fact, Schneier only teaches Bob obtaining d and D directly from Alice and does not include a step of obtaining one component from two

Appl. No. 09/773,665

Reply to Office Action of: September 12, 2005

other components generated by Alice. Schneier is entirely silent in that regard. Moreover, claim 12 requires that the verifier obtain (\bar{s}, r) from (r, s, c) . Schneier does not have an equivalent step. Applicant believes that the Examiner has taken steps performed by Alice and steps performed by Bob in an attempt to find steps that could be considered similar to those recited in claim 12. Applicant believes that even taking a "bit from here" and a "bit from there", Schneier still fails to teach what is recited in claim 12.

Secondly, each step in claim 12 relies in part from what is previously recited in the claim. For example, verifying $r'=r$ requires calculating r' from one of the coordinate pairs, which are recovered using (\bar{s}, r) etc. Applicants believe that they have shown above that Schneier does not teach deriving (\bar{s}, r) as recited in claim 12. Accordingly, Schneier fails to teach any of the steps recited in claim 12 for at least that reason.

Thirdly, the Examiner admits that Schneier does not teach recovering a coordinate pair using, in part the component pair (\bar{s}, r) . However, the Examiner then states that: "Koyama discloses the use of elliptic curve to calculate digital signatures and therefore the recovering of a coordinate pair $(x1, y1)$...". Applicant believes that such a leap of logic is improper, and in fact, the Examiner does not even provide an explanation as to where Koyama provides any direction or motivation to jump from the mere presence of "elliptic curves" to incorporating an undisclosed step into the teachings of Schneier relating to a specific signature scheme. Neither Schneier nor Koyama teach recovering a coordinate pair that corresponds to a short term public key kP using a pair of signature components. Applicants believe that they have shown above that Schneier clearly does not teach obtaining a pair of components (\bar{s}, r) from components (r, s, c) as recited in claim 12. Therefore, even if a person skilled in the art were to combine the teachings of Koyama with Schneier, the result would be a random application of elliptic curve cryptography to the Guillou-Quisquater Signature Scheme without any direction for how to implement a scheme as recited in claim 12, let alone provide any motivation to do so.

Finally, according to MPEP 2143, in order to establish a *prima facie* case of obviousness, the references, when combined, must teach every element recited in the claim and there must be found, some motivation in the teachings to either combine the teachings or modify at least one of the teachings to arrive at what is claimed. Applicant respectfully submits that neither of these criteria has been met.

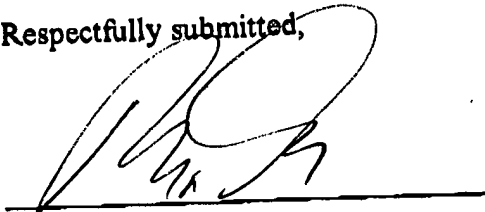
Therefore, Applicant believes that claim 12 clearly distinguishes over the prior art cited

Appl. No. 09/773,665
Reply to Office Action of: September 12, 2005

by the Examiner, and as such is in condition for allowance. Claims 13-21 being ultimately dependent on claim 12 are also believed to distinguish over the prior art.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



Ralph A. Dowell
Agent for Applicant
Registration No. 26,868

Date: MARCH 9, 2006

DOWELL & DOWELL, P.C.
Suite 406, 2111 Eisenhower Avenue
Alexandria, VA 22314
USA

Tel: 703-415-2555
JRO/BSL

Best Available Copy